EXHIBIT 112

PUBLIC

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
ALEXANDIA DIVISION

UNITED STATES OF AMERICA, et al., Plaintiffs, v. GOOGLE, LLC, Defendant.	Case No. 1:23-cv-00108 (LMB/JFA) HON. LEONIE H. BRINKEMA

REBUTTAL EXPERT REPORT OF DR. WENKE LEE
Feb 13, 2024

IV. Mr. Ferrante's failure to consider critical aspects of digital advertising technologies and systems leads him to conclusions that have no factual or scientific support and that are incorrect.

12. Fraud and malicious activity directed against digital advertising is a concern for advertisers, publishers, consumers, and other participants in the digital advertising ecosystem. Fraudulent and malicious activities can harm the integrity of online advertising campaigns, harm participants in the digital advertising ecosystem, skew performance metrics, and siphon advertising spending and profits away from honest and reputable participants in the system.

13. In addressing this important concern generally, and in describing Google's efforts to help develop industry standards to address malvertising and advertising fraud, and to assist efforts to combat specific cybersecurity threats, Mr. Ferrante does not describe, or quantify, Google's overall contributions to increasing cybersecurity protections against malvertising and digital advertising fraud, or state how much those contributions have reduced malvertising and advertising fraud in the digital advertising ecosystem. Nor does Mr. Ferrante compare Google's contributions to the contributions of other industry participants, or state how much, in comparison to others' contributions, Google's contributions have reduced malvertising and advertising fraud.

14. Without such assessments and comparisons, Mr. Ferrante has no basis for evaluating the impact of the contributions to digital advertising security that he identifies Google as having made.

15. In addition, to conduct a reliable analysis of the extent to which advertising technologies and systems, including Google's, have increased security against fraudulent and malicious activity, or the extent to which such technologies and systems are more or less effective than others, , Mr. one would have to fully consider the multiple critical and complex aspects of the digital advertising ecosystems in question, and those of their component technologies, and the potential vulnerabilities those complexities create.[2]

[2] The term "digital advertising ecosystem" refers to the technological infrastructure and systems involved in the delivery, management, and optimization of online advertisements. This ecosystem encompasses a range of technological components, including ad servers, ad networks, demand-side platforms (DSPs), supply-side platforms (SSPs), data management platforms (DMPs), and various analytics and tracking tools. which are described in more detail in Appendix D.

advertisers to identify and prevent domain spoofing. He has not considered any other factor that might influence whether increased advertising bids from publishers would, by themselves, necessarily increase "noise" in requests that would make it more difficult for advertisers to identify and prevent domain spoofing.

108. Without having conducted a comprehensive analysis of the numerous factors that affect the security of Header Bidding systems and the larger ecosystems in which they operate, Mr. Ferrante has no scientific or factual basis for asserting, based solely on the increased volume of bid requests, that Header Bidding systems necessarily make it more difficult for advertisers to identify and prevent domain spoofing, or necessarily increase the vulnerabilities in, or decrease the security of, such systems.

Mr. Ferrante also fails to consider the extent to which publishers and advertisers apply well-known and effective defenses to the known problem of domain spoofing.

109. Publishers and advertisers rely on effective and readily available countermeasures to counteract any potential tendency of Header Bidding to reduce the security of their platforms. These include, for example, widely adopted industry standards such as ads.txt[91] as well as app-ads.txt,[92] sellers.json,[93] and OpenRTB SupplyChain,[94] all of which are useful in preventing fraud by allowing publishers, resellers and advertisers in a bidding transaction to verify and confirm each other's identities. The importance of adopting ads.txt in reducing and combating spoofing is well documented in industry reports; in fact, ads.txt is widely credited as a critical factor in the takedowns of 3ve and Methbot operations.[95] All publishers and advertisers have access to these

[91] "Ads.txt – Authorized Digital Sellers," IAB Tech Lab, last modified July 27, 2020, https://www.iabtechlab.com/ads-txt/.

[92] App-ads.txt is an "extension of the original ads.txt standard to meet the requirements for software applications distributed through mobile app stores." *See* "Authorized Sellers for Apps (app-ads.txt)," IAB Tech Lab, March 2019, https://iabtechlab.com/wp-content/uploads/2019/03/app-ads.txt-v1.0-final-.pdf.

[93] Sellers.json enables "buyers to verify the entities who are either direct sellers of, or intermediaries in the selected digital advertising opportunity for purchase." *See* "Sellers.Json," IAB Tech Lab, last modified July 27, 2020, https://iabtechlab.com/sellers-json/.

[94] OpenRTB SupplyChain allows "buyers to see all parties who are selling or reselling a given bid request." *See* "Sellers.Json," IAB Tech Lab, last modified July 27, 2020, https://iabtechlab.com/sellers-json/.

[95] "2018-2019 Bot Baseline Report," White Ops and ANA, accessed February 12, 2024, https://www.ana.net/miccontent/show/id/rr-2019-bot-baseline, at 5.

industry-wide standards, which are engineered so that they do not get "overwhelmed" by the volume of bid requests.[96]

110. Advertisers additionally use pre- and post-bid verification mechanisms to analyze the efficacy of the inventory on which they run impressions.[97,98] As I describe above, these standards are not unique to Google. Any SSP and DSP can access and read the file to verify domain authenticity. Thus, there is also no reason DSPs and SSPs that adopt Header Bidding systems cannot implement countermeasures to domain spoofing that are similar to or more effective than the countermeasures against domain spoofing that Google could implement.

111. Mr. Ferrante also does not consider other, non-technical countermeasures to prevent domain spoofing in connection with the use of Header Bidding. These include choosing to receive bid requests from Supply Side Platforms ("SSPs") offering better domain spoofing protections. He also fails to consider that advertisers could reduce the number of sources of bid requests if the human reviewers at their DSPs are overwhelmed. Mr. Ferrante also does not evaluate whether and to what extent DSPs have been successful in identifying and thwarting domain spoofing through technical and other means without human intervention.

112. Because Mr. Ferrante does not consider these factors, there is no basis for his assertion that the "noise" from the multiple bid requests generated by Header Bidding made it more difficult for advertisers to identify and prevent domain spoofing.

---

[96] The mechanism by which ads.txt works is that brands and advertisers can crawl specific domains to see which publishers have an ads.txt file under their domain. Once a brand or advertiser has a list of publishers that use ads.txt, they can reference this list against IDs in partner bid requests. In computer programming, checking a database for even hundreds of thousands bid requests is very fast and easily automated. For more information, *see* Maciej Zawadzinski and Mike Sweeney, "What is Ads.txt and How Does it Work?," Clearcode, November 09, 2017, https://clearcode.cc/blog/ads-txt/.

[97] "Pre-bid/Post-bid Verification: What are your options?," Blis, accessed February 12, 2024, https://blis.com/pre-bid-post-bid-verification-options-location-based-campaigns/.

[98] "TAG Fraud U.S. Benchmark Study," The 614 Group and Trustworthy Accountability Group, November 2020, https://f.hubspotusercontent40.net/hubfs/2848641/614_008_US%20Benchmark%20Report%202020_007.pdf, at 8.